UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/557,628	11/17/2005	Pim Theo Tuyls	NL030552	4463

24737 7590 02/18/2010

PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
SIMS, JING F	

ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
02/18/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/557,628	TUYLS ET AL.	
	Examiner	Art Unit	
	JING SIMS	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 October 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communications: application 10/557,628 filed on 11/17/2005; RCE amendment filed on 10/12/2009.

2. Claims 1, 2, 4-6, 14-18 are amended.

Response to Arguments

8. Applicant's arguments with respect to claims 1 and 14 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 1-6, 14-18 are rejected under 35 U.S.C 103(a) as being unpatentable over Yamaguchi et al (US Patent no.: 6314196, hereinafter Yamaguchi), in view of Zhao et al. (US Patent Application Pub. No.: US 2004/0125993).

As per claim 1, Yamaguchi discloses:

"a method of generating authentication data for authenticating a physical object; the method comprising acts of" *(col. 1, line 7-8, a fingerprint registering method for registering a fingerprint; col. 1, line 32-33, to authenticate personal identification)*; and

"a computer program stored on a computer readable memory device for generating authentication data for authenticating a physical object, the computer program being operative to cause a processor to" (fig. 45, and col. 10, line 7-15, the fingerprint checking device includes a processor, a read-only memory storing a program, a multivalued image memory, a binarized image memory):

"measuring a property set Y of the object using a measurement procedure" (col. 18, lines 53-57, wherein fingerprint image of a fingerprint corresponding with property set Y of the object; also fig. 1, ref. no. 1, Yamaguchi discloses this limitation as "fingerprint image pickup unit" a fingerprint image is property set, and the pickup unit certainly performing a measurement procedure to pickup the fingerprint);

"creating a property set I from the measured property set Y that meet a predetermined robustness criterion" (col. 18, lines 58, wherein the digitized/binarized fingerprint image corresponding with property set I; col. 4, lines 27-33, describe the criteria to digitize the image; it also shows in fig. 1, ref. 10, property set I appears to be the data that after binarized image converting unit process);

"creating a property set A from the property set I that includes less information on the actual properties than property set Y" (col. 18, lines 61-63, wherein the binarized fingerprint image after thinning-processed corresponding to property set A; col. 2, lines 8-14, the thinning process, also in fig. 32 B, the binarized fingerprint image after thinning process shows less distracting information than the original fingerprint image in fig. 32A), "wherein the creating acts are guided by a criteria W" (col. 18, lines 61-63, wherein the thinning process corresponding with criteria W, or col. 4, lines 27-33, and

line 52-61, Fig. 36, the creating acts are guided by a criteria W as m and/or n. M and n control the selection of the subsets which are the divided image blocks. Thereby limit the range of parameters (finger print pattern) which is the criteria that guides the creating acts);

"generating a control value V in dependence on properties of property set A (fig. 2, ref. no. A11, control value V appears to be the best finger selection. The best fingerprint selection is based on result after thinning);

However, Yamaguchi does not explicitly disclose:

"storing the control value V and the criteria together as the generated authentication data to a storage device, wherein the criteria is not a member of property sets utilized for generating the control value V".

Zhao discloses:

"storing the control value V and the criteria together as the generated authentication data to a storage device" (fig. 16, steps 670 and 680; see also page 7, [0083], lines 1-7, the fingerprint features and score threshold are stored in memory; wherein fingerprint feature corresponding with control value V, and Score threshold corresponding with criteria) , "wherein the criteria is not a member of property sets utilized for generating the control value V" (fig. 16, steps 640 and 650; see also [0082], the match score threshold is chosen based up the level of security required, which discloses the threshold is not the fingerprint data itself but information to help generating a value for fingerprint enrollment process).

Yamaguchi and Zhao are analogous art because they are from the same field of endeavor of a processing and authenticating biometric information such as fingerprints.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the fingerprint registering method as described by Yamaguchi and add the final value of the registered or enrolled fingerprint stored also with a criteria that help to generate the final value during the registration or enrollment process as taught by Zhao, because it would provide a system the choice of score threshold to able user chose the level of security. For example, a banker may require higher level security while a cell phone user may desire relatively low level of security (see Zhao, page 7, [0082], and lines 12-17).

As per claim 2, Yamaguchi discloses "the method as claimed in claim 1, wherein the act of creating the property set A includes performing a contracting transformation that transforms given ranges of input properties to corresponding output values" (Fig. 3, ref. no. B4, Yamaguchi discloses as "extract minutiae". The process of "extracting minutiae" is to transform a biometric data - for example a fingerprint - from one state to the other state by performing "extract minutiae". The input properties range is the thinning processed image and the output values are the minutiae are the detected minutia based on the thinning processed image in col. 20, line 61-63).

However, Yamaguchi does not disclose the transforms are guided by the criteria.

Zhao discloses "the transforms are guided by the criteria" (page 7, [0082]).

As per claim 3, Yamaguchi discloses "the method as claimed in claim 1, wherein the contracting transformation transforms a property to a binary number representative of whether the property has a positive or negative value" (Fig. 17, ref. no. A8, and col. 29, line 7-8 "the content d at the n-th byte of the registered fingerprint data is stored in the register (A8)" Yamaguchi discloses the content in "byte", it is the length unit used by binary numbers, and therefore, "a property" is represented by binary numbers. Transforming a property to binary number representative of whether the property has a positive or negative value is well known technology in the art, for example, US Patent 3,947,876 discloses "to convert the positive and negative data transitions to binary ones and zeros respectively" (see Gary, col. 7, line 50-54).

As per claim 4, Yamaguchi discloses "the method as claimed in claim 1, wherein the act of creating the property set A includes an act of selecting a subset of the property set I" (col. 4, line 27-30 and line 52-61, Yamaguchi discloses an self-explanatory diagram in Fig. 36, Yamaguchi also explains "dividing a pictured image into blocks, and when 512.times.512 picture elements are determined as one screen, division into 1024 blocks is made with 16.times.16 picture elements as one block"; therefore, the blocks have the equal meaning with "subsets" in the instant application. Yamaguchi further discloses "selecting a subset" as in Fig. 38, and give the example of "the flowchart of a conventional example". It is an actually selecting process of subsets in Yamaguchi's application).

However, Yamaguchi does not disclose the process is guided by the criteria.

Zhao discloses the process is guided by the criteria (page 7, [0082]).

As per claim 5, Yamaguchi discloses "the method as claimed in claim 4, including an act of creating criteria for controlling the selection" (col. 4, line 27-33, and line 52-61, Fig. 36 are an self-explanatory diagram of dividing a pictured image into blocks, the subset has been described as blocks "in which a block number is initialized with m=1 (B-1). In other words, number m for 1 to 1024 is allocated with respect to 1024 blocks in the image shown in FIG. 36, and the block number m is determined as 1 for initialization. Then, with n=1 (B2), the picture element number n in the block is initialized. In other words, the number n for 256 picture elements in the image shown in FIG. 36 is allocated, and this picture element number n is determined as 1 for initialization." Yamaguchi discloses the "criteria W" in the application appears to be m or/and n. M and n controls the selection of the subsets which are the divided image blocks. Thereby limit the range of parameters (finger print pattern) which is the criteria that controls the selection).

As per claim 6, Yamaguchi discloses "the method as claimed in claim 5, including an act of creating criteria based on respective authentication applications" (col. 3, line 57-67, Yamaguchi discloses "based on the multivalued image, it is judged by the fingerprinting judging unit 313" "division into respective blocks is made". Yamaguchi discloses earlier "block number m and picture element number n", so m is block number. It indicates from above statements that the block number m is based on the

multivalued image. The multivalued image is generated upon the fingerprint by the fingerprint image pickup unit 311. Therefore, the block number m is uniquely created respect to each authentication applications), "wherein different respective authentication applications have different unique criteria" (m and n are variables. The example in col. 4, line 52-61, m has been set to 1-1024, and n has been set to 1-256; however, Yamaguchi also discloses the criteria can be changed due to different applications in col. 4, line 5-8, as the process of determining the luminance of the focused picture element can be made with respect to blocks. In col. 3, line 64-67, it indicates the block can be 16x16 or others, which indicates the criteria/variables m and n may be changed based on the luminance of each application).

As per claim 14, claim 14 is a computer program claim corresponding to the method claim 1 and therefore is rejected under the same reasons set forth in the rejections for claim 1.

As per claim 15, Yamaguchi discloses:

"a method of authenticating a physical object; the method comprising acts of: measuring a property set Y of the object using a measurement procedure; creating a property set I from the measured property set Y that meet a predetermined robustness criterion; creating a property set A from the property set I that includes less information on the actual properties than property set Y; generating a control value V' in dependence on properties of the property set A". The limitations above are identical to

the corresponding section of generating authentication data in claim 1. They are rejected under the same reasons set forth in the corresponding rejections for claim 1.

Yamaguchi also discloses “retrieving a control value V (col. 19, lines 52-56, checking unit fetches the registered best fingerprint) and criteria W (col. 22, lines 1-6, since the fingerprint checking unit and the fingerprint registering device have a common function in the processing the fingerprint, they can be achieved by the same computer, therefore, the finger checking unit must retrieve same thinning process function as the registering process) that has been generated for the physical object during an enrollment wherein the creating acts are guided by the criteria; and authenticating the physical object if there is a predetermined correspondence between the generated control value V' and the retrieved control value V” (col. 30, line 25-35, in Fig. 20, flowchart of registering of the register “first fingerprint” in ref. no. A2, and by authenticating the physical object by “match” in ref. no. A5. “The first fingerprinting is effected" means the process of retrieving a control value V. "A predetermined correspondence” are explained as “to judge whether or not they match” in prior art. It discloses “the authentication may in principle be done using the same apparatus as used for the enrollment” in the specification. Fig. 20 in Yamaguchi’s application is the example of this model).

However, Yamaguchi does not disclose:

“wherein the act of retrieving comprises an act of retrieving the control value V and the criteria together from a storage device”, and “wherein the criteria is not a member of property sets utilized for generating the control values V, V'”;

Zhao discloses:

"wherein the act of retrieving comprises an act of retrieving the control value V and the criteria together from a storage device" (fig. 3, steps 340 and 350; see also page 5, [0068], lines 1-8, the degree of the similarity between a air of search and file fingerprint minutiae is quantified in terms of an output match score; wherein the control V corresponding with file print), and "wherein the criteria is not a member of property sets utilized for generating the control values V, V'" (fig. 3, steps 340 and 350; see also page 5, [0068], wherein file print corresponding with the control V, and search print corresponding with control value V'; fig. 16, steps 640 and 650; see also [0082], the match score threshold is chosen based up the level of security required, which discloses the threshold is not the fingerprint data itself but information to help generating a value for fingerprint enrollment process).

Yamaguchi and Zhao are analogous art because they are from the same field of endeavor of a processing and authenticating biometric information such as fingerprints.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the fingerprint registering method as described by Yamaguchi and add the final value of the registered or enrolled fingerprint stored also with a criteria that help to generate the final value during the registration or enrollment process as taught by Zhao, because it would provide a system the choice of score threshold to able user chose the level of security. For example, a banker may require higher level security while a cell phone user may desire relatively low level of security (see Zhao, page 7, [0082], and lines 12-17).

As per claim 16, Yamaguchi discloses

"a computer program stored on a computer readable memory device for authenticating a physical object, the computer program being operative to cause a processor to" (fig. 45, and col. 10, line 7-15, the fingerprint checking device includes a processor, a read-only memory storing a program, a multivalued image memory, a binarized image memory):

measure a property set Y of the object using a measurement procedure; create a property set I from the measured property set Y that meet a predetermined robustness criterion; create a property set A from the property set I that includes less information on the actual properties than property set Y; generating a control value V' in dependence on properties of property set A". The limitations above are identical to the corresponding section of generating authentication data in claim 1. They are rejected under the same reasons set forth in the corresponding rejections for claim 1.

Yamaguchi also discloses "retrieving a control value V (col. 19, lines 52-56, checking unit fetches the registered best fingerprint) and criteria W (col. 22, lines 1-6, since the fingerprint checking unit and the fingerprint registering device have a common function in the processing the fingerprint, they can be achieved by the same computer, therefore, the finger checking unit must retrieve same thinning process function as the registering process) that has been generated for the physical object during an enrollment, wherein the creating the property set I and the property set A are guided by the criteria"; "and authenticating the physical object if there is a predetermined

correspondence between a generated control value V' and the retrieved control value V" (col. 30, line 25-35, in Fig. 20, flowchart of registering of the register "first fingerprint" in ref. no. A2, and by authenticating the physical object by "match" in ref. no. A5. "The first fingerprinting is effected" means the process of retrieving a control value V. "A predetermined correspondence" are explained as "to judge whether or not they match" in prior art. It discloses "the authentication may in principle be done using the same apparatus as used for the enrollment" in the specification. Fig. 20 in Yamaguchi's application is the example of this model).

However, Yamaguchi does not disclose:

"wherein the act of retrieving comprises an act of retrieving the control value V and the criteria together from a storage device", and "wherein the criteria is not a member of property sets utilized for generating the control values V, V'";

Zhao discloses:

"wherein the act of retrieving comprises an act of retrieving the control value V and the criteria together from a storage device" (fig. 3, steps 340 and 350; see also page 5, [0068], lines 1-8, the degree of the similarity between a air of search and file fingerprint minutiae is quantified in terms of an output match score; wherein the control V corresponding with file print), and "wherein the criteria is not a member of property sets utilized for generating the control values V, V'" (fig. 3, steps 340 and 350; see also page 5, [0068], wherein file print corresponding with the control V, and search print corresponding with control value V'; fig. 16, steps 640 and 650; see also [0082], the match score threshold is chosen based up the level of security required, which

discloses the threshold is not the fingerprint data itself but information to help generating a value for fingerprint enrollment process).

Yamaguchi and Zhao are analogous art because they are from the same field of endeavor of a processing and authenticating biometric information such as fingerprints.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the fingerprint registering method as described by Yamaguchi and add the final value of the registered or enrolled fingerprint stored also with a criteria that help to generate the final value during the registration or enrollment process as taught by Zhao, because it would provide a system the choice of score threshold to able user chose the level of security. For example, a banker may require higher level security while a cell phone user may desire relatively low level of security (see Zhao, page 7, [0082], and lines 12-17).

As per claim 17, Yamaguchi discloses:

"a system for authenticating a physical object" (col. 17, line 3-4, Yamaguchi discloses "the embodiment of a fingerprint checking device") "the system including an enrollment device" (Fig. 1, ref. no. 1 Yamaguchi discloses as "image pickup unit"); "an authentication device" (Fig. 1, ref. no. 1, Yamaguchi discloses as "image pickup unit". The specification of the instant application discloses that the authentication may in principle be done using the same apparatus as used for the enrollment, therefore, authentication device also can be "image pickup unit") "and a storage for storing authentication data" (Fig. 1, reference unit 6, Yamaguchi discloses as "registering unit",

it also can be find in Fig. 20, ref. no. A3, Yamaguchi discloses as “temporary fingerprint registering”);

“the enrollment device including: an input for receiving a property set Y of the object measured using a measurement procedure” (fig. 1, ref. no. 1, fingerprint image pickup unit);

“a processor for creating a property set I from the measured property set Y that meet a predetermined robustness criterion” (col. 18, lines 58, wherein the digitized/binarized fingerprint image corresponding with property set I; col. 4, lines 27-33, describe the criteria to digitize the image; it also shows in fig. 1, ref. 10, property set I appears to be the data that after binarized image converting unit process), “creating a property set A from the property set I that includes less information on the actual properties than property set Y” (col. 18, lines 61-63, wherein the binarized fingerprint image after thinning-processed corresponding to property set A; col. 2, lines 8-14, the thinning process, also in fig. 32 B, the binarized fingerprint image after thinning process shows less distracting information than the original fingerprint image in fig. 32A), “wherein the creating the property set I and the property set A are guided by a criteria” (col. 18, lines 61-63, wherein the thinning process corresponding with criteria W, or col. 4, lines 27-33, and line 52-61, Fig. 36, the creating acts are guided by a criteria W as m and/or n. M and n control the selection of the subsets which are the divided image blocks. Thereby limit the range of parameters (finger print pattern) which is the criteria that guides the creating acts); “and generating a control value V in dependence on properties of the property set A and the criteria” (fig. 2, ref. no. A11, control value V

appears to be the best finger selection. The best fingerprint selection is based on result after thinning. Best fingerprint also depends on the thinning process); and

"the authentication device including":

"an input for receiving a property set Y' of the object measured using a measurement procedure and for receiving the control value V and criteria together from the storage; a processor for creating a property set I' from the measured property set Y' that meet a predetermined robustness criterion; for creating a property set A' from the property set I' that includes less information on the actual properties than property set Y', wherein the creating the property set I' and the property set A' are guided by the criteria W; for generating a control value V' in dependence on properties of the property set A'" (since the specification of the instant application discloses that the authentication may in principle be done using the same apparatus as used for the enrollment, therefore, see the rejection to claims 1 or 15, for the corresponding sections); "for authenticating the physical object if there is a predetermined correspondence between the generated a control value V' and the retrieved control value V and an output for issuing a signal indicating whether or not the physical object has been authenticated" (Fig. 1, reference 5, "checking unit" and/or "judging unit"; fig. 20, ref. no. A5, the issued signal appears to be the signal after the process of match).

However, Yamaguchi does not explicitly disclose "output the criteria W to a storage device and part of the authentication data", and "wherein the criteria is not a member of property sets utilized for generating the control values V, V'".

Zhao discloses:

"an output for supplying the control value V and the criteria to the storage together as the authentication data" (fig. 16, steps 670 and 680; see also page 7, [0083], lines 1-7, the fingerprint features and score threshold are stored in memory; wherein fingerprint feature corresponding with control value V, and Score threshold corresponding with criteria); and

"wherein the criteria is not a member of property sets utilized for generating the control values V, V'" (fig. 3, steps 340 and 350; see also page 5, [0068], wherein file print corresponding with the control V, and search print corresponding with control value V'; fig. 16, steps 640 and 650; see also [0082], the match score threshold is chosen based up the level of security required, which discloses the threshold is not the fingerprint data itself but information to help generating a value for fingerprint enrollment process).

Yamaguchi and Zhao are analogous art because they are from the same field of endeavor of a processing and authenticating biometric information such as fingerprints.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the fingerprint registering method as described by Yamaguchi and add the final value of the registered or enrolled fingerprint stored also with a criteria that help to generate the final value during the registration or enrollment process as taught by Zhao, because it would provide a system the choice of score threshold to able user chose the level of security. For example, a banker may require higher level security while a cell phone user may desire relatively low level of security (see Zhao, page 7, [0082], and lines 12-17).

As per claim 18, Yamaguchi discloses:

"an authentication device for authenticating a physical object, the authentication device comprising" (col. 17, line 3-4, Yamaguchi discloses "the embodiment of a fingerprint checking device"):

"an input for receiving a property set Y of a physical object measured using a measurement procedure" (Fig. 1, ref. no. 1, fingerprint image pickup unit);

"a processor for creating a property set I from the measured property set Y that meet a predetermined robustness criterion" (col. 18, lines 58, wherein the digitized/binarized fingerprint image corresponding with property set I; col. 4, lines 27-33, describe the criteria to digitize the image; it also shows in fig. 1, ref. 10, property set I appears to be the data that after binarized image converting unit process), "for creating a property set A from the property set I that includes less information on the actual properties than property set Y" (col. 18, lines 61-63, wherein the binarized fingerprint image after thinning-processed corresponding to property set A; col. 2, lines 8-14, the thinning process, also in fig. 32 B, the binarized fingerprint image after thinning process shows less distracting information than the original fingerprint image in fig. 32A), "wherein the creating the property set I and the property set A are guided by a criteria W" (col. 18, lines 61-63, wherein the thinning process corresponding with criteria W, or col. 4, lines 27-33, and line 52-61, Fig. 36, the creating acts are guided by a criteria W as m and/or n. M and n control the selection of the subsets which are the divided image blocks. Thereby limit the range of parameters (finger print pattern) which is the criteria

that guides the creating acts); “for generating a control value V’ in dependence on properties of the property set A” (fig. 2, ref. no. A11, control value V appears to be the best finger selection. The best fingerprint selection is based on result after thinning); “and for authenticating the physical object if there is a predetermined correspondence between the generated a control value V' and the retrieved control value V and an output for issuing a signal indicating whether or not the physical object has been authenticated” (Fig. 1, reference 5, "checking unit" and/or “judging unit”; fig. 20, ref. no. A5, the issued signal appears to be the signal after the process of match).

However, Yamaguchi does not disclose:

“Receiving a control value V and a criteria together from a storage” and “wherein the criteria is not a member of property sets utilized for generating the control values V, V'”;

Zhao discloses:

“Receiving a control value V and a criteria together from a storage” (fig. 3, steps 340 and 350; see also page 5, [0068], lines 1-8, the degree of the similarity between a air of search and file fingerprint minutiae is quantified in terms of an output match score; wherein the control V corresponding with file print), and

“wherein the criteria is not a member of property sets utilized for generating the control values V, V'” (fig. 3, steps 340 and 350; see also page 5, [0068], wherein file print corresponding with the control V, and search print corresponding with control value V’; fig. 16, steps 640 and 650; see also [0082], the match score threshold is chosen based up the level of security required, which discloses the threshold is not the

fingerprint data itself but information to help generating a value for fingerprint enrollment process).

Yamaguchi and Zhao are analogous art because they are from the same field of endeavor of a processing and authenticating biometric information such as fingerprints.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the fingerprint registering method as described by Yamaguchi and add the final value of the registered or enrolled fingerprint stored also with a criteria that help to generate the final value during the registration or enrollment process as taught by Zhao, because it would provide a system the choice of score threshold to able user chose the level of security. For example, a banker may require higher level security while a cell phone user may desire relatively low level of security (see Zhao, page 7, [0082], and lines 12-17).

11. Claims 7, 9, 10 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over anticipated by Yamaguchi (US 2001/6314196), in view of Ort et al. (US 5799098) (hereinafter Ort).

As per claim 7, Yamaguchi discloses “the method as described in claim 1”, but fails to disclose "wherein the predetermined robustness criterion is based on a signal to noise ratio of the measured properties and the act of creating the property set I includes performing a transformation .GAMMA. on the property set Y to create two disjunct property sets I.sub.1 and I.sub.2 where a signal to noise ratio of properties of the

property set I.sub.1 are estimated to be higher than a signal to noise ratio of properties of I.sub.2; and using I.sub.1 as the property set I."

However, Ort discloses the limitations (col. 14, line 29-41, Ort uses "filter 110" and "filter 120" to serve the functionalities of transformation Γ. "The two disjunct property set I.sub.1 and I.sub.2" are described as the output data I.sub.FSCE after the process of contrast enhancement in fig. 7, ref. no. 120 and the output data I.sub. FS after the process of low pass filter (Fig. 7 ref. no. 110 respectively. It is obvious for one skilled in the art to observe that I.sub.FSCE has higher Signal to noise ratio than the output data I.sub. FS after the process of low pass filter in Fig. 7 reference 110 and the purpose of this transformation is to produce a higher signal to noise ratio.)

Yamaguchi and Ort are analogous art because they are from the same field of using biometric data, which in both applications are fingerprints to enhance the image of fingerprint quality by eliminating the noise, and get a higher signal to noise ratio.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teaching of Yamaguchi to use the low filter and contrast enhancement of Ort because it would provide to enforce the robust criterion, then to further consolidate the security of the system by applying the techniques to lessen the contained information in Yamaguchi.

As per claim 9, Ort discloses "the method as claimed in claim 7, including the act of creating the transformation .GAMMA. in dependence on a statistical property of the measurement procedure" (col. 14, line 28-41, Ort discloses the statistical property in

the term of "high frequency noise". The high frequency noise data is obviously generated during the measurement procedure.)

As per claim 10, Ort discloses "the method as claimed in claim 9, wherein the statistical property includes a covariance matrix derived from estimated properties X of the object and a corresponding statistical distribution F determined during the measuring the property set Y" (col. 14, line 20-41, Ort discloses estimated properties X to be "ridge angle", and corresponding statistical distribution F appears to be "an 800 by 800 pixel image". It is obvious for one skilled in the art that both of the data sets are represented by matrices. The 800 by 800 pixel image is determined during the measuring of the original physical object).

As per claim 11, Ort discloses "the method as claimed in claim 7, including an act of deriving a threshold from a noise level in the measured property set and assigning created properties with an absolute value larger than the threshold to set I.sub.1" (col. 29, line 43-50, with respect to this limitation, Ort discloses "The 256 cells of Q.sub.coarse are filled by sequentially considering the data within each of 256 16.times.16 cell submatrices of Q.sub.smooth that in total comprise all the cells of it. Each of the 16 cells within a submatrix is examined to determine if the stored cell value is below a fixed poor quality threshold. If 75% of the cells are below a quality of 0.5 for Q.sub.coarse, then the cell is dubbed as poor quality. If 75% (12 cells) are below the threshold then: the corresponding Q.sub.coarse (i, aj) is set to 0; otherwise Q.sub.coarse (i, j) is set to 1." Ort discloses the same concept of deriving a threshold from the percentage of measured property set by using the term "Q.sub.coarse").

12. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Yamaguchi, in view of Ort, and further in view of Vizcaya (Pedro Vizcaya, A personnel identity verification method using DAB fingerprints (Pattern recognition), 1998).

As per claim 8, Yamaguchi and Ort disclose a method as claimed in claim 7 but do not specifically teach wherein the transformation .GAMMA. is a linear transformation that converts a vector representing the property set Y to a vector with components as representing the set I, where each vector component .alpha..sub.i is independent of the other vector components .alpha...sub.j (j.noteq.i) and wherein the vector components are sorted according to an estimated signal to noise ratio.

However, Vizcaya discloses "a linear transformation" (Page ix, line 19-23, "a linear transformation" by "since model is linear, its parameters are efficiently calculated using standard linear transform techniques. Additionally, the model allows the evaluation of the specific contribution of each singularity to explain the ridge orientation everywhere") "that converts a vector representing the property set Y to a vector with components as representing the set I, where each vector component .alpha...sub.i is independent of the other vector components .alpha..sub.j (j.noteq.i) and wherein the vector components are sorted according to an estimated signal to noise ratio" Using independent vectors with sorted order to represent a physical object (i.e. property set) is well known and expected in the art.

Yamaguchi, Ort, and Vizcaya are all analogous art because they are all from the same field of enhancing the biometric data, which in these three cases specifically fingerprints, by extracting the key feature to get a higher signal to noise ratio, to authenticate an access.

It would have been obvious to one of ordinary skill in the art at the invention time to modify the teaching of Yamaguchi in view of Ort for applying the linear transformation algorithm of Vizcaya because it would provide for the transformation of a vector to the other vectors in more rapid fashion, therefore, to shorten the authentication processing time.

13. Claims 12 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yamaguchi in view of Bjorn (US 6035398).

As per claim 12, Yamaguchi discloses “the method as claimed in claim 1, wherein the act of creating the control value V” [see rejection to claim 1 above], and “converting each property of the property set A into a binary digit” (transforming a property to binary number representative of whether the property has a positive or negative value is well known technology in the art, for example, US Patent 3,947,876 discloses "to convert the positive and negative data transitions to binary ones and zeros respectively" (see Gary, col. 7, line 50-54)), but fails to disclose “includes acts of performing a cryptographic function on properties of the property set A”.

However, Bjorn discloses “performing a cryptographic function on a combination of the binary digits” (col. 4, line 25-37, and Fig. 3, ref. no. 325, Hash template to create

cryptographic key, at block 325, "the template is hashed. For one embodiment, this hash is the cryptographic key. For another embodiment, known techniques are used on the hash to generate the cryptographic key. This cryptographic key is identified with the specific fingerprint, and thus with a specific user". It is known that cryptographic function is performed on combination of the binary code at the invention time).

Yamaguchi and Bjorn are analogous art because they are from the same field of using biometric data to enhance authentication process.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teaching of Yamaguchi to apply the one-way hash function of Bjorn because it would provide to generate a cryptographic key to enhance the security of control value V in Yamaguchi for the authentication.

As per claim 13, Bjorn discloses claim 13 "the cryptographic function is a one-way function" (col. 4, line 25-37, and Fig. 3 ref. no. 325 Hash template to create cryptographic key, at block 325, the template is hashed. For one embodiment, this hash is the cryptographic key. For another embodiment, known techniques are used on the hash to generate the cryptographic key. This cryptographic key is identified with the specific fingerprint, and thus with a specific user").

Examiner Notes

14. Examiner has pointed out particular references contained in the prior arts of record and in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the

specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable to the limitations of the claims. It is respectfully requested from the applicant, in preparing for response, to consider fully the entire reference as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the Examiner.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, THIS ACTION IS MADE FINAL. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JING SIMS whose telephone number is (571)270-7315. The examiner can normally be reached on 7:30am-5:00pm EST, Mon-Thu.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/JING SIMS/
Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437